Secure Spectrum Sensing In Cognitive Radio Sensor Networks: A Survey

Laila Nassef [1, 2] , Reemah Alhebshi [1]

[1] Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia
[2] Department of Computer Sciences and Information, Institute of Statistical Studies and Research, Cairo University, Egypt

Abstract

The rapid growth in wireless communications has contributed to a huge demand on the deployment of new wireless services in both the licensed and unlicensed frequency spectrum. Cognitive Radio Networks (CRNs) is a recently emerging paradigm that aim to opportunistically access the intermittent periods of unoccupied frequency bands and therefore increasing the spectral efficiency. Unlike conventional radios, cognitive radios can intelligently adjust their transmission/reception parameters based on the interaction with the environment and find the best available spectrum bands to use. CRNs rely on cooperation for much of their functionality to make network more efficient. However, due to the distributed nature of cooperative spectrum sensing, the network is vulnerable to new types of security threats. The current spectrum sensing methods do not provide security mechanism to mitigate against these attacks. Traditional security solutions for non-cognitive wireless networks do not work well when they are confronted with these new attacks. Furthermore, the security mechanisms proposed for cognitive radio ad hoc networks are not applicable for resource constrained cognitive radio sensor networks. These present considerable obstacles to development of a security mechanism that can defend against such attacks. This paper investigates threats and defense mechanism applicable for cognitive radio sensor networks to use the proposed guidelines for future development of a security mechanism for cognitive radio sensor networks.

Keywords: *Cognitive Radio Networks (CRNs), Dynamic Spectrum Access (DSA), Cognitive Radio Sensor Networks (CRSNs), Security mechanism.*

I. Introduction

Wireless Sensor Networks (WSNs) [1] consists of spatially distributed autonomus sensors that monitor a wide range of ambient conditions and cooperate to share data across the network. WSNs enable a wide range of applications in both military and civilian domains such as battlefield surveillance, medical monitoring, biological detection, home security, smart grid, inventory tracking, etc. [2]. These sensors perform a collaborative measurement process using small, low-cost, resource-limited (battery, bandwidth, processing, memory) nodes that communicate wirelessly and cooperate to forward data in a multi-hop fashion. The majority of WSNs operate in the unlicensed 2.4 GHz Industrial Scientific and Medical (ISM) band, where other wireless technologies operate as well. As a result, the wireless spectrum has become congested in the unlicensed bands and WSNs suffer from severe interference from other networks sharing the same ISM spectrum. Furthermore, the harsh and complex environmental conditions, dynamic topology changes, connectivity problems, interference, and fading, make wireless communication very challenging [3]. Consequently, there is a need for the next generation of WSNs that utilize the advantages of Cognitive Radio (CR) technology [4].

CR has opened up a new way of sensing and utilizing precious wireless spectrum resources by sensing the spectrum and using its free portions, called White Spaces (WSs) [5], in an opportunistic manner [6]. WSs are the frequency bands assigned to the licensed users, called Primary User (PUs). At a particular time and specific geographic location, the band reserved for PUs is not being utilized. CR dynamically reconfigurable the radio devices to be able of learn and adapt to their surrounding environment by adjusting their transmitting waveform, channel access method, spectrum use, and networking protocols as needed to achieve optimum network performance [7]. These capabilities have been become feasible by using recent advances of Software Defined Radio (SDR) and smart antennas [8]. Cognitive Radio Networks (CRNs) have the ability for self-programming which is achieved through the methodology of “understanding by building” to achieve two primary objectives, which are permanent reliable communications and efficient utilization of the spectrum resources [9].

Cognitive Radio Ad Hoc Networks (CRAHNs) [10] is proposed to solve the problems of spectrum scaricy in Mobile Ad hoc NETworks (MANETs) to deploy highly reconfigurable and self organizing networks. It mainly focused on the development of efficient spectrum sensing and selection techniques for unlicensed users called Secondary Users (SUs) that can communicate without interfering with the transmissions of PUs. CRAHNs do not consider the energy efficiency and network lifetime of WSNs.

Cognitive Radio Sensor Network (CRSN) [11] is defined as a distributed network of cognitive radio wireless sensor nodes, which sense an event signal and collaboratively communicate their readings dynamically over the available spectrum bands in a multi hop manner, ultimately to satisfy the application specific requirements. CRSNs can communicate in a wide range of spectrum bands by changing its transmission parameters dynamically during network communication in response to the changes in the sensed spectrum environment and the signals received from other sensor nodes [12]. This Dynamic Spectrum Access (DSA) [13] is a very promising spectrum efficient communication paradigm in CR. It allows SUs to operate in the best available, without degrading performance of PUs. This may happen in time, frequency, and space domains.

The realization of CRSNs require an efficient spectrum management framework to regulate the DSA to find the spectrum opportunity. Therefore, the individual SU should undergo through a cognitive cycle, illustrated in Figure 1, with the following phases [9]:

1) *Spectrum sensing:* to determine which portions of the spectrum is available and to detect the presence of PUs.

2) *Spectrum decision:* to select the best available spectrum channel, based on the availability of the spectrum and other policies.

3) *Spectrum sharing:* to coordinate access to this channel among SUs to provide a fair and optimal spectrum allocation method among them.

4) *Spectrum mobility:* to vacate the channel when a PU is detected and move to next best available spectrum band.

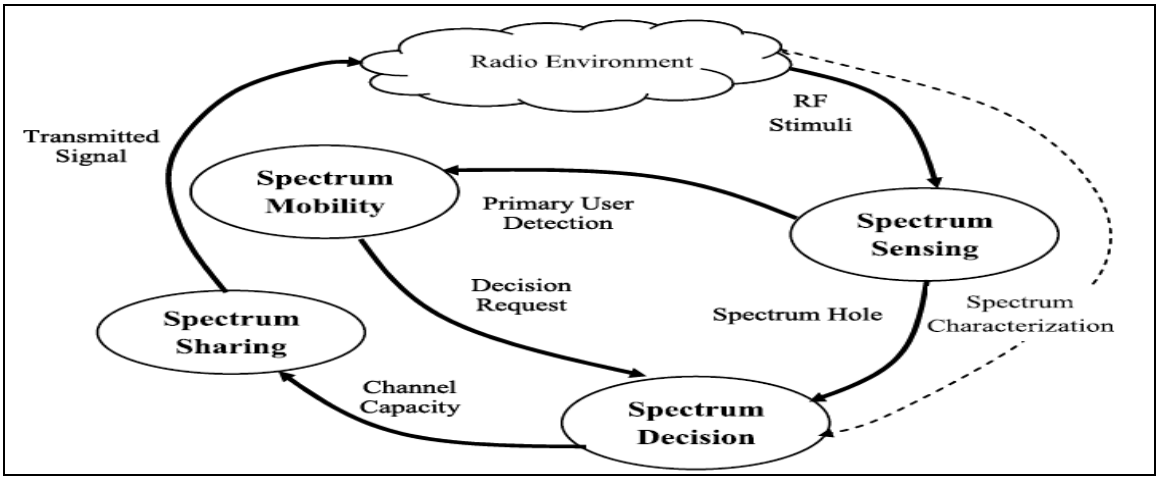

Figure 1. The cognitive cycle implemented by each SU

Spectrum sensing is the main function of DSA, which can be implemented using various methods based on matched filter, energy detection, cyclostationary detection, wavelet detection and covariance detection [14]. Existing spectrum sensing methods can be classified as non-cooperative and cooperative sensing. Non-cooperative sensing exploit the physical layer characteristics of PU transmissions such as energy, matched filter, and cyclostationary features [9]. Cooperative sensing improve upon non-cooperative sensing by allowing the exchange of spectrum sensing information between multiple CRs to detect PU. CSS can be implemented as either centralized, distributed, or relay-assisted sensing [15]. The performance of spectrum sensing is affected by noise uncertainties, shadowing, and multi-path fading effects [9] when the received PU's signal to noise ratio is too low. Cooperative Spectrum Sensing (CSS) improves the reliability of spectrum sensing and the utilization of WSs [16] compared with the non-cooperative spectrum sensing. CSS are divided into three categories: censoring, clustering, and user selection, and can be implemented as centralized or distributed [17]. In centralized CSS, a central controller collects sensing reports from multiple SUs, decides the spectrum occupancy, by using decision fusion rules, then informs the SUs which channels to access. In distributed CSS [18], SUs exchange their sensing reports among themselves without requiring a backbone or centralized infrastructure. Among the four different phases of cognitive cycle, spectrum sensing is important from security point of view since it is most vulnerable to attacks. The current spectrum sensing methods do not provide security mechanism to mitigate against these attacks, especially for CRSNs.

CRs are naturally based on artificial intelligent techniques which give them the ability to be aware of the surrounding RF environment through perception (process of knowing) to identify the ongoing RF activities [19]. CRs also have the ability of learning and reasoning. Learning is the ability to create knowledge from the collected sensing reports. It implies that the current actions are based on past and current observations of the environment. Reasoning is ability to use that knowledge acquired through learning to achieve the required objectives. These capabilities have been made feasible through the use of SDR and cognitive cycle defined previously, where a cognitive engine coordinates the actions by applying machine learning and reasoning algorithms. CRNs actually integrating concepts from artificial intelligence and wireless networking sciences [19].

This paper is organized as follows. Section 2 provides security threats and defense mechanisms for WSN. Section 3 provides security threats and defense mechanisms for cognitive radio sensor networks. Section 4 states conclusion and future works.

II. Cognitive Radio Sensor Networks

The open nature of the wireless communication, the lack of infrastructure, the fast deployment practices, and the hostile deployment environments, make WSNs vulnerable to a wide range of security attacks targeting the control or data traffic. However, the open nature of the wireless communication, the lack of infrastructure, the fast deployment practices, and the hostile deployment environments, make WSNs vulnerable to a wide range of security attacks targeting the control or data traffic. Typical examples of control traffic are routing, monitoring (whether a node is awake, asleep, or dead), topology discovery, and distributed location determination [20]. Control traffic attacks include the Wormhole attack [21], the Rushing attack [22], the Sybil attack [23], the Sinkhole attack [24], and the HELLO flood attack [25]. Control attacks are dangerous because they can be used to interrupt functionality of the various protocols and create opportunities for a malicious node to launch data traffic attacks such as dropping all or a selective subset of data packets. In addition to control traffic attacks, WSNs are also vulnerable to data traffic attacks such as Blackhole attack [26], selective forwarding and artificially delaying of packets [27], in which respectively a malicious node drops data (entirely or selectively) passing through it, or delays its forwarding. The attacks could result in a significant loss of data or degradation of service.

Numerous techniques and solutions for traditional network’s security that prevent attacks or contain the extent and damage of such attacks [28]. There are many techniques used to defend against WSNs attacks with most important methods used is cryptography. Cryptography is a method of storing and transmitting data so that only the authorized entity can read and process it. There are two type of encryption techniques; symmetric key and public (asymmetric) key. In symmetric key cryptography, the communicating parties exchange a secrete key that is used for both encryption and decryption of the message. Asymmetric key cryptographic has two different keys that are used for encryption and decryption. For encryption, a public key is used to encrypt the message, and for decryption, the private key is used to decrypt the message [29].

Several random key predistribution schemes have been proposed for symmetric encryption techniques [30]. In public key cryptography techniques, an efficient mechanism for public-key distribution is necessary as well [31]. These traditional techniques come at the cost of computation complexity of encryption algorithms, memory usage for storing security information, and network bandwidth for key synchronization and certificate distribution and revocation [32], which often cannot be satisfied by resource-constrained WSNs. There is some research found solutions to overcome resource constrained in WSNs. An overview of some representative energy efficient security techniques presented in [33], and the most common security protocols that used in WSN. In [34] a comparison between asymmetric encryption algorithms in WSN is illustrated, and has been found that RSA public key algorithm is the most commonly used and achieved good efficiency. An optimized computation for RSA in WSN implemented in [35]. The main constraint in RSA is that it needs a high processing power and memory resources. For that, authors changed the packet format of the message by adding an extra identification field, and modified the ASCII code to suite the RSA implementation.

WSNs require every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to WSN’s security. For example, pre installing a shared key between the base station and all sensors is inhibited [36]. Therefore, traditional network security solutions cannot be directly applied to WSNs. The attacks against WSNs are getting sophisticated, and hence pose a significant challenge for designing secure WSNs. In the same way that distributed sensor networks must be self-organize to support multihop routing, they must also self-organize to perform key management and build trust relation among sensors.

The open, unattended, and physically insecure environments, where an attacker can easily capture nodes and subsequently use these nodes, make network vulnerable to compromise. Sensors can be modified to misbehave and interrupt the network operation. This allows the attacker to access the cryptographic material held by the captured node and allow the attacker to launch attacks from within the system as an insider, bypassing encryption and password security techniques. Even though cryptography can provide integrity, confidentiality, and authentication, it fails in the face of insider attacks [37]. This necessitates a solution that can cope with such internal attacks.

Trust can solve some problems of using the traditional cryptographic security. However, it is not easy to build a good trust model within a sensor network because of its resource limitations. Furthermore, in order to keep the sensor nodes independent, trust among sensors must be known in advance. Some work have been proposed recently to propose a reputation based framework for high integrity WSNs [38] to employ a beta reputation system for reputation representation, updates, and integration. In [39], a mechanism of location centric isolation of misbehaving nodes for trust routing in WSNs is proposed. If the trust value is below a specific trust threshold, then this location is considered insecure and is avoided when forwarding packets.

III. Security Threats to Cognitive Radio Sensor Networks

From the security point of view, all security threats that target WSN's authenticity, confidentiality, integrity, availability and access control do exist in CRSNs [40]. Apart from these traditional threats, several new security threats that are mainly related to two fundamental characteristics: cognitive capability, and reconfigurability are introduced for both CRNs and CRAHNs [41]. These threats may potentially challenge the main goal of network, which is the usage of the available radio spectrum space in a fair and optimal way, while preserving PUs from interferences. Furthermore, these attacks can not be defended by traditional security mechanisms of WSNs [42] or currently proposed techniques for CRNs and CRAHNs. The detection of these type of attacks is a difficult problem. First, the channel shadowing and fading result in spatial variability and uncertainty of the PU signal, and hence the sensing reports among geographically separated SUs are usually distinct. This makes it easy for attacker to hide the dishonest sensing reports under the natural variation of the sensing reports. Second, due to the open and easy reconfiguration nature of CR, the SUs are more prone to be compromised and once compromised, they are prone to more misbehaviors. CRSNs have unique challenges due to: the inherent resource constraints of sensor nodes, additional communication and processing demand imposed by CR capabilities, low power efficient CR sensor nodes, multihop and cooperative communications over licensed and unlicensed spectrum bands. All are challenges to the development of a security mechanism for CRSNs.

The cooperation among SUs introduce entirely new types of security vulnerabilities to wireless networks in general and WSNs in particular. Some of the threats that are related to the cognitive capabilities [42] are:

1. *Primary User Emulation Attack (PUEA):* in which attacker mimic features of PU transmissions such as power, modulation type, synchronization sequences etc., or by recording and replaying PU transmissions, in order to force other SUs to vacate or avoid using specific frequency bands and consequently cause the disruption of the network's operations and unfairness on spectrum sharing.
2. *Spectrum Sensing Data Falsification Attack (SSDF):* also known as Byzantine attack, in which attacker reports false spectrum sensing data to the neighbors or to a base station and affects the effectiveness of spectrum decision, and
3. *Location Privacy Attack (LPA):* in which attacker intercept signals and sensing reports (may involve different strategies such as: eavesdropping, impersonation, and traffic analysis) so that it can extract sensitive information to launch more powerful attacks.

To mitigate these attacks, a SU must possess four key characteristics. First, it has to possess the ability to make authentication for the local nodes forming the CRSN. Second, it has to be able to exchange information with other SUs in a strongly secure way. Third, it has to validate the information exchanged among the different SUs. Last and not least, it has to be able to analyze the behavior of the different nodes of network.

In non-cognitive wireless networks, countermeasures mainly focus on increasing the signal's robustness to attacks, by reaching agreements between the transmitters and the receivers, such as encryption, authorization and authentication [43]. However, in CRNs, the SU system requires no significant modifications to the PU system and they are generally separated without signaling exchange. This isolation between the PU and the SUs make the countermeasures that are used in traditional networks, invalid for CRNs and act as a major limited condition in designing effective defense schemes against spectrum sensing attacks [44].

For the successful deployment of CRSNs and the realization of their benefits, essential security mechanisms must be deployed in sufficiently robust form to resist misuse of the networks. Conventional cryptographic mechanisms such as authentication and encryption can provide data confidentiality, data integrity and node authentication for exchanged reports and protect the network from external attacks. A legitimate node can act selfishly, and refuse to participate in order to save its energy resources and maximize its own performance, or it can act maliciously and impair the network. These types of threats, which are introduced by cooperative process, are known as internal attacks where cooperating SUs owning legitimate cryptographic keys. However, and to the best of our knowledge, there is no research papers deal with these type of attacks using cryptographic mechanisms.

CRs are naturally based on artificial intelligent techniques, which give them ability of learning and reasoning [19]. Different types of learning paradigms have been found in literature. These algorithms are usually categorized as supervised (learning by instruction) or unsupervised (learning by reinforcement) [45]. Supervised learning such as support vector machine and artificial neural networks are generally used in certain known environments with prior knowledge about the characteristics of the environment [46]. On the other hand, unsupervised learning such as reinforcement learning (RL), Bayesian non parametric approaches, and game theory are particularly applicable for CRNs [47]. In RL, CR without having any prior knowledge is trained period to learn from its own experience by evaluating the feedback signals that it receives after each action. RL relies on its interactions with the environment and tries to learn on its own interacts to learn autonomously without supervision. RL approaches are trial and error, dynamic programing, temporal difference and the joined approach found in Q-learning algorithm [48].

In [49], a distributed Q-learning algorithm is proposed for CRSNs to implement channel selection and power control jointly, which takes channel state as the input and takes the selected channel and transmit power as the output. This adaptive spectrum decision of channel choice and power control with distributed Q-learning can be extended to add security aspects in the decision process of CRNs to against a jamming attacks [50].

On the other hand, game theory is a mathematical tool that implements the behavior of rational entities in an environment of conflict [51]. It has been applied to communication networks to model and analyze routing and resource allocation in competitive environments. A game theory model consists of several players and each player has a set of available actions and a utility function. The utility function of an individual player depends on the actions taken by all the players. Each player selects its strategy (action sequence) in order to maximize its utility function. Several types of games have been used in CRNs to model different conditions [52]; such as repeated games, stochastic games, and evolutionary games. For example, repeated games were used for DSA by multiple SU's that share the same spectrum [53]. It was used to build reputations and applying punishments in order to reinforce a certain desired outcome. A Nash equilibrium [51] of a game is the point at which the utility function of each player does not increase if the player deviates from that point, given that the other players' actions are fixed. The basics of the auction games and the open challenges of auction games to the field of spectrum management are provided in [54]. Stochastic games [51], which are generalizations of repeated games that only have one single state, was used to model the greedy selfish behavior of SUs in CRNs, where SUs try to learn their best response and improve their strategies over time, the stochastic games are dynamic, competitive games with probabilistic actions played by SU's. Applying game theoretic solutions to CRNs has advantageous in reducing the complexity of adaptation algorithms [53].

Several learning models for CRNs based on Markov Model, Q-learning, fuzzy logic, genetic algorithms, neural networks, and game theory have been proposed to mitigate the security challenges in CRNs [47]. They make advantageous of common feature of both learning and cognition.

Abnormality detection algorithm based on proximity has been proposed in [55], to solve the problem of malicious SUs using history reports of each SU. Reputation evaluation system has been proposed in [56], in which a node's confidence in its spectrum sensing report is used as a weight during calculation of spectrum decisions. The calculation of the trust of SUs has been addressed using different techniques.

Among other techniques, the Bayesian rule [57] is applied to compute the posteriori probability of being an attacker for each SU. When the posteriori probability of a certain SU exceeds the suspicious level threshold, it is claimed to be an attacker and is removed from the cooperation.

Game theory [54] is also used as an effective framework for the design of security mechanisms, since it provides analytical tools to predict the outcome of interactions among rational entities with conflicting interests that compete for the limited network resources (i.e. Spectrum and/or energy). A game theoretic framework in [58] has studied the PUEA where a non-cooperative game between the legitimate SUs and malicious SUs is formulated. Pure-strategy and mixed strategy Nash equilibrium of the game have been investigated between legitimate and malicious SUs. Game theory is also used to implement the reputation systems [59] to quantify the trust of SUs to validate the data by using qualitative or evidence based quantitative measures. In [60], a game-theoretic approach to analyze SUs' behavior is proposed with direct and indirect punishments. SUs are prevented from SSDF by setting appropriate reward and punishment functions. A framework for securing CRNs has been proposed in [61], which can be used to propose secure CRSNs.

IV. Conclusion

The current cooperative spectrum sensing methods do not provide security mechanism to mitigate against the new types of attacks introduced by cognitive cycle. On the other hand, CRSNs have unique challenges due to the inherent resource constraints of sensor nodes, additional communication and processing demand imposed by CR capabilities, low power efficient CR sensor nodes, multihop and collaborative communications over licensed and unlicensed spectrum bands. All are challenges to the development of such security mechanism. Moreover, the existing techniques for traditional WSNs are not applicable for that dynamic environment. Furthermore, the security mechanisms developed for CRNs and CRAHNs can not be used for resource constrained CRSNs. To the best of our knowledge, there is no work studied security aspects of the cooperative spectrum sensing in cognitive radio sensor networks. This paper presented the motivation for the development of a security mechanism that is designed especially for CRSNs and raised specific attention to security of resource constrained cognitive radio sensor networks. Our future work is to developed a threat model to define particular attack(s) for cooperative spectrum sensing and then propose an intelligent security mechanism that can defend against such attack(s). The performance of the proposed security defense mechanism will be validated through simulations.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, p. 393–422, 2002, Volume: 38, Issue: 4, PII: S13 8 9-1 2 86 (0 1) 0 03 0 2- 4.

[2] K. Sohraby, D. Minoli and T. Znati, Wireless Sensor Networks: Technology, Protocols, and Applications, New Jersey, USA: A John Wiley & Sons, INC., Publication, 2007, pp. ISSN: 2231-2307.

[3] G. P. Joshi, S. Y. Nam and S. W. Kim, "Cognitive Radio Wireless Sensor Networks:Applications, Challenges and Research Trends," Sensors, pp. 11196-11228., 2013, Volume: 13, DOI:10.3390/s130911196.

[4] J. Mitola and G. Q. Maguire, "Cognitive Radio: Making Software Radios More Personal," Personal Communications, IEEE, pp. 13 - 18, 06 August 1999, Volume: 6, Issue: 4, DOI: 10.1109/98.788210.

[5] K. G. Shin, H. Kim, A. W. Min and A. Kumar, "Cognitive Radios For Dynamic Spectrum Access: From Concept To Reality," Wireless Communications, IEEE Magazines, pp. 64 - 74, 23 December 2010, Volume: 17, Issue: 6, DOI: 10.1109/MWC.2010.5675780.

[6] E. Arun and V. Catherine, "Relay Based Cooperation for Cognitive Radio Networks," International Journal of Signal System Control and Engineering Application, pp. 1-9, 2011. Volume: 4; Issue: 1, DOI: 10.3923/ijssceapp.2011.1.9.

[7] "Cognitive Radio: Brain-Empowered Wireless Communications," IEEE Journal on Selected Areas in Communications, pp. 201 - 220, 07 February 2005, Volume: 23, Issue: 2, DOI: 10.1109/JSAC.2004.839380.

[8] "Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS)," ITU-R Report SM 2152, Geneva, Switzerland, 2009.

[9] I. F. Akyildiz, B. Lo and R. Balakrishnan, "Cooperative Spectrum Sensing in Cognitive Radio Networks: A Survey," Physical Communication, p. 40–62, 2011, Volume: 4, Issue: 1, DOI:10.1016/j.phycom.2010.12.003.

[10] I. F. Akyildiz, W. Lee and K. R. Chowdhury, "CRAHNs: cognitive radio ad hoc networks," Ad Hoc Networks, p. 810–836, 2009, Volume: 7, Issue: 5, DOI:10.1016/j.adhoc.2009.01.001.

[11] O. B. Akan, O. B. Karli and O. Ergul, "Cognitive Radio Sensor Networks," IEEE Network, pp. 34 - 40, 2009, Volume: 23, Issue: 4, DOI: 10.1109/MNET.2009.5191144.

[12] A. Ghasemi and E. Sousa, "Collaborative Spectrum Sensing for Opportunistic Access in Fading Environments," First IEEE International Symposium onNew Frontiers in Dynamic Spectrum Access Networks (DySPAN), pp. 131 - 136, November 2005, DOI: 10.1109/DYSPAN.2005.1542627.

[13] I. F. Akyildiz, W. Y. Lee, M. C. Vuran and S. Mohanty, "Next Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks:A Survey," Computer Networks, p. 2127–2159, Septemper 2006, Volume: 50, Issue: 13, DOI:10.1016/j.comnet.2006.05.001.

[14] R. K. Dubey and G. Verma, "Improved Spectrum Sensing for Cognitive Radio Based on Adaptive Threshold," in Second International Conference on Advances in Computing and Communication Engineering (ICACCE), Dehradun, 1-2 May, 2015, DOI: 10.1109/ICACCE.2015.70.

[15] W. Lee and I. F. Akyildiz, "A Spectrum Decision Framework for Cognitive Radio Networks," IEEE Transactions on Mobile Computing, pp. 161 - 174, 17 December 2011, Volume: 10, Issue: 2, DOI: 10.1109/TMC.2010.147.

[16] S. Parvin, F. K. Hussain, O. K. Hussain, S. Han, B. Tiana and E. Chang, "Cognitive radio network security: A survey," Journal of Network and Computer Applications, p. 1691–1708, 27 June 2012, Volume: 35, DOI.org/10.1016/j.jnca.2012.06.006.

[17] X. Zhang, X. Liu, H. Samani and B. Jalaian, "Cooperative Spectrum Sensing in Cognitive Wireless Sensor Networks," International Journal of Distributed Sensor Networks, 13 April 2015, Article ID 170695, http://dx.doi.org/10.1155/2015/170695.

[18] K. Letaief and W. Zhang, "Cooperative communications for cognitive radio networks," Proceedings of the IEEE, pp. 878 - 893, 12 May 2009, Volume: 97, Issue: 5, DOI: 10.1109/JPROC.2009.2015716.

[19] A. He, K. K. Bae, T. R. Newman, J. Gaeddert, K. Kim, R. Menon, L. Morales-Tirado, J. J. Neel, Y. Zhao, J. H. Reed and W. H. Tranter, "A Survey of Artificial Intelligence for Cognitive Radios," IEEE Trans. Veh. Technol., pp. 1578 - 1592, 27 May 2010, Volume: 59, Issue: 4, DOI: 10.1109/TVT.2010.2043968.

[20] I. Khalil, S. Bagchi, C. Rotaru and N. Shroff, "UNMASK: Utilizing Neighbor Monitoring for Attack Mitigation in Multihop Wireless Sensor Networks," Ad Hoc Networks, Elsevier, 12 June 2009, doi:10.1016/j.adhoc.2009.06.002.

[21] J. Zhou, "Efficient and Secure Routing Protocol Based on Encryption and Authentication for Wireless Sensor Networks," International Journal of Distributed Sensor Networks, 2013, Article ID 108968, http://dx.doi.org/10.1155/2013/108968.

[22] Y.-C. Hu, A. Perrig and D. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," WiSe '03 Proceedings of the 2nd ACM workshop on Wireless security, pp. 30-40, 2003, DOI: 10.1145/941311.941317.

[23] K. Abirami and B. Santhi, "Sybil attack in Wireless Sensor Network," International Journal of Engineering and Technology (IJET), pp. 620-623, Apr-May 2013, Volume: 5, Issue: 2, ISSN : 0975-4024.

[24] S. A. Salehi, M. A. Razzaque, P. Naraei and A. Farrokhtala, "Detection of Sinkhole Attack in Wireless Sensor Networks," IEEE International Conference on Space Science and Communication (IconSpace), pp. 361 - 365, 2013, DOI: 10.1109/IconSpace.2013.6599496.

[25] "A Survey in Hello Flood Attack in Wireless Sensor Networks," International Journal of Engineering Research & Technology, pp. 1882-1887, January 2014, Volume: 3, Issue: 1, ISSN: 2278-0181.

[26] M. Wazid, A. Katal, R. S. Sachan, R. H. Goudar and D. P. Singh, "Detection and prevention mechanism for Blackhole attack in Wireless Sensor Network," International Conference on Communications and Signal Processing (ICCSP), pp. 576 - 581, 2013, DOI: 10.1109/iccsp.2013.6577120.

[27] P. Sharma, M. Saluja and K. K. Saluja, "Analysis of Selective Forwarding Attacks In Wireless Sensor Networks," International Journal of Computer Applications, pp. 10-14, July 2012, Volume: 49, Issue: 17, http://dx.doi.org/10.5120/7718-1082.

[28] P. Niksaz and M. J. Kargar, "A Full Review of Attacks and countermeasures in Wireless Sensor Networks," International Journal of Information Security And Privacy, pp. 1-39, October-December 2012. Volume: 6, Issue: 4, DOI: 10.4018/jisp.2012100101.

[29] W. Stallings, Cryptography and Network Security: Principles and Practice, Sixth Edition, USA: Pearson Education, Inc. , Jun, 2013.

[30] X. Zhang , H. Heys and C. Li, "Energy Efficiency of Symmetric Key Cryptographic Algorithms in Wireless Sensor Networks," in 25th Biennial Symposium on Communications (QBSC), Kingston, 12-14 May 2010, DOI: 10.1109/BSC.2010.5472979.

[31] A. Kaur, "Energy Analysis of Wireless Sensor Networks using RSA and ECC Encryption Method," International Journal of Scientific & Engineering Research, pp. 2212-2216, May 2013. Volume: 4, Issue: 4, ISSN 2229-5518.

[32] G. Sharma, S. Bala and A. K. Verma, "Security Frameworks for Wireless Sensor Networks-Review," Procedia Technology, p. 978 – 987, 2012, Volume: 6, DOI: 10.1016/j.protcy.2012.10.119.

[33] K. Daniluk and E. Niewiadomska-Szynkiewicz, "A Survey of Energy Efficient Security Architectures and Protocols for Wireless Sensor Networks," Journal of Telecommunications and Information Technology, pp. 64-72, 3 2012.

[34] G. S. Quirino, A. R. Ribeiro and E. D. Moreno, "Asymmetric Encryption in Wireless Sensor Networks," InTech, Science, Technology and Medicine open access publisher., pp. 217-232, 06 Septemper 2012, DOI: http://dx.doi.org/10.5772/48464.

[35] Sridevi, "Security Protocol For Sensor Network Using RSA," International Journal of Computer Science and Mobile Computing (IJCSMC), pp. 297-305, June 2014, Volume: 3, Issue: 6, ISSN 2320–088X.

[36] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme For Distributed Sensor Networks," in 9th ACM conference on Computer and communications security, New York, USA, 2002, DOI: 10.1145/586110.586117.

[37] S. K. Singh, M. P. Singh and D. K. Singh, "A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks," International Journal of Computer Trends and Technology (IJCTT), May to June 2011, ISSN: 2231-2803.

[38] S. Ganeriwal, L. K. Balzano and M. B. Balzano, "Reputation-Based Framework For High Integrity Sensor Networks," ACM Transactions on Sensor Networks (TOSN), May 2008, Volume: 4 Issue: 3, DOI: 10.1145/1362542.1362546.

[39] T. Sapon, P. Dave, R. Bhindwale and A. Helmy, "Location-Centric Isolation of Misbehavior and Trust Routing In Energy-Constrained Sensor Networks," IEEE International Conference on Performance, Computing, and Communications, pp. 463 - 469, February 2004, DOI: 10.1109/PCCC.2004.1395061.

[40] A. G. Fragkiadakis, E. Z. Tragos and I. G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks," Communications Surveys & Tutorials, IEEE Journals & Magazines, pp. 428 - 445, 05 February 2013, Volume: 15, Issue: 1, DOI: 10.1109/SURV.2011.122211.00162.

[41] Z. Qin, Q. Li and G. Hsieh, "Defending Against Cooperative Attacks In Cooperative Spectrum Sensing," IEEE Transactions on Wireless Communications, pp. 2680 - 2687, 27 June 2013, Volume: 12, Issue: 6, DOI: 10.1109/TWC.2013.041913.120516.

[42] A. Fragkiadakis, V. Angelakis and E. Z. Tragos, "Securing Cognitive Wireless Sensor Networks: A Survey," International Journal of Distributed Sensor Networks, Hindawi Publishing Corporation. Article ID 393248, pp. 1-12, 2014, doi.org/10.1155/2014/393248.

[43] K. Venkatraman, J. V. Daniel and G. Murugaboopathi, "Various Attacks in Wireless Sensor Network: Survey," International Journal of Soft Computing and Engineering (IJSCE), pp. 208-211, March 2013. Volume: 3, Issue: 1, ISSN: 2231-2307.

[44] A. Araujo, J. Blesa, E. Romero and D. Villanueva, "Security in Cognitive Wireless Sensor Networks. Challenges and Open Problems," EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, 2012, DOI: 10.1186/1687-1499-2012-48.

[45] D. Vernon, Artificial Cognitive Systems: A Primer, USA: Massachusetts Institute Technology (MIT) Press, 2014.

[46] L. Wang, Support Vector Machines: Theory and Applications, Netherland: Springer Science & Business Media, 2005.

[47] N. Abbas, Y. Nasser and K. El Ahmad, "Recent advances on artificial intelligence and learning techniques in cognitive radio networks," EURASIP Journal onWireless Communications and Networking, 2015, DOI 10.1186/s13638-015-0381-7.

[48] C. WATKIN and P. DAYAN, "Technical Note Q-Learning," Kluwer Academic Publishers, pp. 279-292, 1992. Volume: 8, DOI 10.1186/s13638-015-0381-7.

[49] J. He, J. Peng, F. Jiang, G. Qin and W. Liu, "A Distributed Q Learning Spectrum Decision Scheme for Cognitive Radio Sensor Network," International Journal of Distributed Sensor Networks, 2015, http://dx.doi.org/10.1155/2015/301317.

[50] F. Slimeni, B. Scheers, Z. Chtourou and V. Le Nir, "Jamming Mitigation In Cognitive Radio Networks Using A Modified Q-Learning Algorithm," in International Conference on Military Communications and Information Systems (ICMCIS), Cracow, 2015, DOI: 10.1109/ICMCIS.2015.7158697.

[51] B. Wang, Y. Wu and K. J. Liu, "Game theory for cognitive radio networks: An overview," Computer Networks, Elsevier B.V, pp. 2537 - 2561, 06 April 2010. Volume: 54, Issue: 14, DOI: 10.1016/j.comnet.2010.04.004.

[52] B. BENMAMMAR and F. KRIEF, "Game Theory Applications In Wireless Networks: A Survey," Applications of Information Systems in Engineering and Bioscience, pp. 208-215, 2014, ISBN: 978-960-474-381-0.

[53] M. Bkassiny, L. Yang and S. K. Jayaweera, "A Survey on Machine-Learning Techniques in Cognitive Radio," Communications Surveys & Tutorials, IEEE Journals & Magazines, pp. 1136 - 1159, 31 July 2013, Volume: 15, Issue: 3, DOI: 10.1109/SURV.2012.100412.00017.

[54] Q. Ni, R. Zhu, Z. Wu, Y. Sun, L. Zhou and B. Zhou, "Spectrum Allocation Based on Game Theory in Cognitive Radio Networks," Journal of Networks, pp. 712-722, March 2013, Volume: 8, Issue: 3, DOI: 10.4304/jnw.8.3.712-722.

[55] R. Chen, J. M. Park, Y. T. Hou and J. H. Reed, "Toward Secure Distributed Spectrum Sensing In Cognitive Radio Networks," Communications Magazine, IEEE, pp. 50 - 55, 03 April 2008, Volume: 46, Issue: 4, DOI: 10.1109/MCOM.2008.4481340.

[56] K. Zeng, P. Paweczak and D. Cabri, "Reputation-Based Cooperative Spectrum Sensing With Trusted Nodes Assistance," Communications Letters, IEEE, pp. 226 - 228, 08 March 2010, Volume: 14, Issue: 3, DOI: 10.1109/LCOMM.2010.03.092240.

[57] A. S. Rawat, P. Anand, H. Chen and P. K. Varshney, "Collaborative Spectrum Sensing In The Presence Of Byzantine Attacks In Cognitive Radio Networks," IEEE Transactions on Signal Processing, pp. 774 - 786, 10 January 2011, Volume: 59, Issue: 2, DOI: 10.1109/TSP.2010.2091277.

[58] Y. Tan, S. Sengupta and K. Subbalakshmi, "Primary User Emulation Attack In Dynamic Spectrum Access Networks: A Game Theoretic Approach," Communications, IET Journals & Magazines, pp. 964 - 973, 09 July 2012, Volume: 6, Issue: 8, DOI: 10.1049/iet-com.2010.0573.

[59] T. Zhang, R. Safavi-Naini and Z. Li, "ReDiSen: Reputation-Based Secure Cooperative Sensing In Distributed Cognitive Radio Networks," IEEE International Conference on Communications (ICC), pp. 2601 - 2605, 9-13 June 2013, DOI: 10.1109/ICC.2013.6654927.

[60] S. Alrabaee, A. Agarwal, D. Anand and M. Khasawneh, "Game Theory For Security In Cognitive Radio Networks," International Conference on Advances in Mobile Network, Communication and Its Applications, Bangalore, 2012, DOI: 10.1109/MNCApps.2012.17.

[61] E. Romero, A. Mouradian, J. Blesa, J. Moya and A. Araujo, "Simulation Framework For Security Threats in Cognitive Radio Networks," Communications, IET Journals & Magazines, pp. 984 - 990, 2012, Volume: 6, Issue: 8, DOI: 10.1049/iet-com.2010.0582.